



Legacy STIGs on IASE

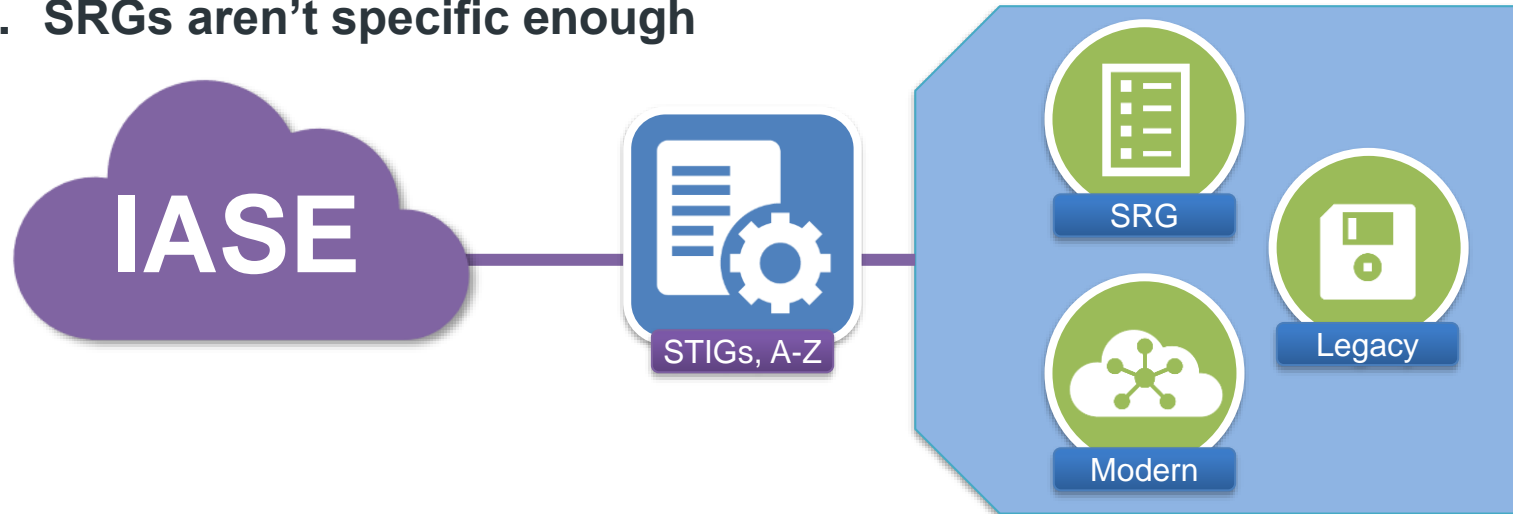
Network STIG Updates

Esteban Banda
DISA RE11, Cyber Standards Branch
May 2019



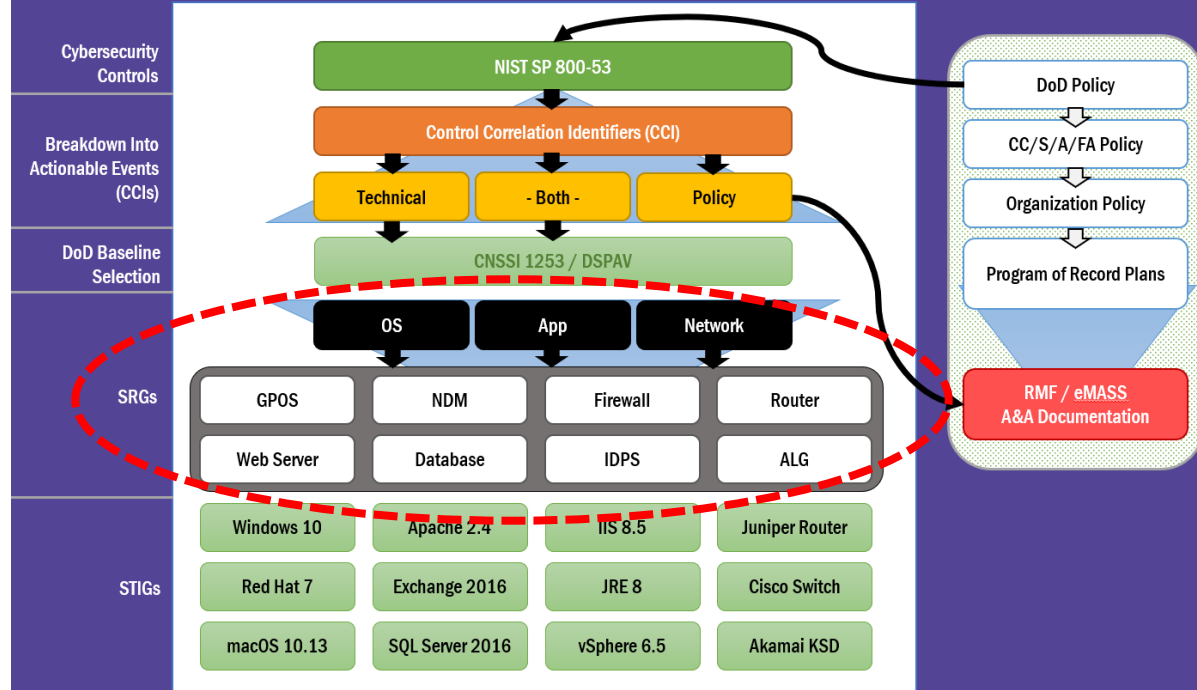
Problem Statements

1. There are 2 kinds of STIGs on IASE: legacy & modern
2. Why don't we just convert legacy STIGs to modern STIGs?
3. What are SRGs? Do they replace STIGs? What's the hierarchy – are SRGs higher or lower than STIGs? Do I need both SRGs and STIGs?
4. SRGs aren't specific enough

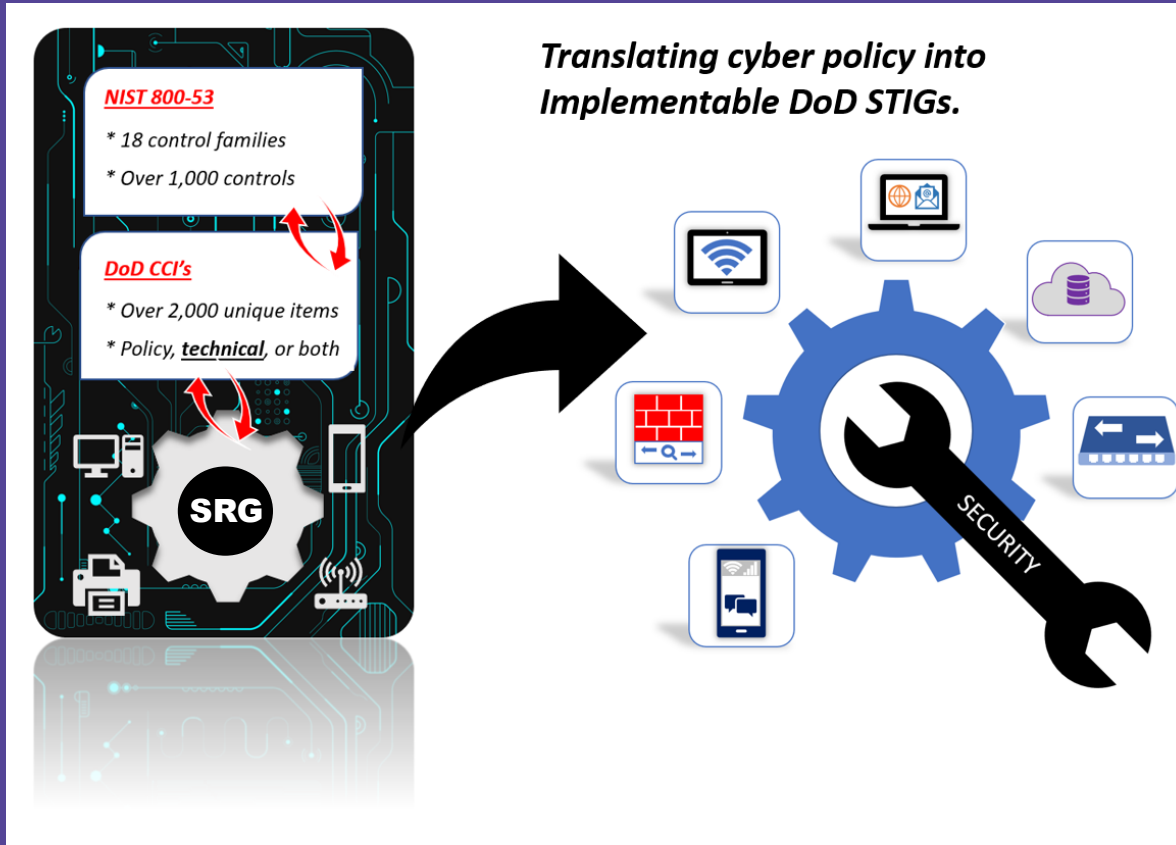


What Are Security Requirements Guides?

- **SRGs are similar to STIGs and are based on NIST SP 800-53 like STIGs**
- **The requirements are actually a subset of minimum baseline requirements, but specific to a technology area**
- **The SRG technology-specific baselines were approved by the DSAWG**



- SRGs shall be used when no product-specific STIG exists
- Because SRGs are tailored by technology, STIGs are derived from SRGs
- SRGs and STIGs are not meant to be used for the same technology (e.g. Router SRG with Cisco Router STIG)





STIGs: Legacy vs. Modern

- **Legacy STIGs were based on [now cancelled] guidance**
 - DoDI 8500.2, “IA Implementation”
 - DoDI 8510.01 “DoD IA Certification and Accreditation Process (DIACAP)”
 - Other: Lots of memos, directives, instructions, CTOs, DTMs, etc.
- **Modern STIGs are based on current guidance**
 - DoDI 8500.01, “Cybersecurity”
 - DoDI 8510.01, “Risk Management Framework for DoD IT”
 - NIST SP 800-53, “Security and Privacy Controls for Federal IT”
 - CNSSI 1253, “Security Categorization and Control Selection for NSS”
 - DoD Specific Assignment Values (DSPAV), RMF Knowledge Service (RMF-KS)






Legacy - Sample STIG

DoDI 8500.2
IAIA-1*

Unique ID	Case Sensitive PW	8 Characters
1 Number	1 Special Char.	
1 Upper Case	1 Lower Case	Remove Default
Change 4+ Char.	Enforce PW Exp.	No Sharing PW
Request In-Person	Supervisor Auth.	No Embedded PW
PW Encrypted St.	PW Encrypted Tr.	Deployed/Tactical

		Title		MAC OS X 10.6 Workstation STIG (2013)	
Vuln ID:		V-29439		Rule ID:	SV-38607r1_rule
STIG ID:		OSX00038 M6		Severity:	CAT II
Rule:		Complex password includes symbol character.			
Check:		Is a special character requirement configured?			
Fix:		Configure a special character requirement.			
IA Control:		IAIA-1			

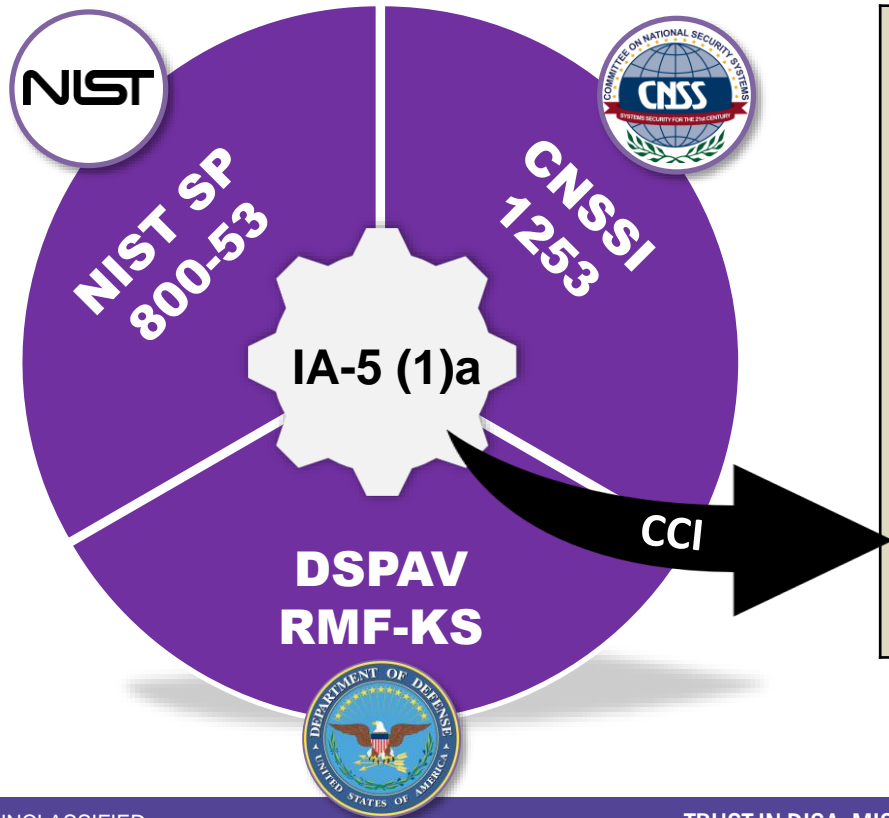


*What about the other IAIA-1 stuff?
What about the 800-53 stuff?
How does the old map to the new?*

* Ref: DoD 8500.2 (cancelled), Identification and Authentication



Modern – Sample STIG



Title	Apple OS X 10.13 STIG (2018)		
Vuln ID:	V-81639	Rule ID:	SV-96353r1_rule
STIG ID:	AOSX-13-000587	Severity:	CAT II
Rule:	The macOS system must enforce password complexity by requiring that at least one special character be used.		
Check:	Is a special character requirement configured?		
Fix:	Configure a special character requirement.		
IA Control:	CCI-001619 NIST SP 800-53 Rev 4 :: IA-5 (1) (a)		



Modern STIG – Cybersecurity Source



REFERENCES

DoD Policy :

DoDI 8500.01
DoDI 8510.01

DoD Cybersecurity Controls :

NIST SP 800-53

NSS/DoD Baseline Selection :

CNSSI 1253

NSS Baseline Values :

CNSSI 1253

DoD Enhanced Values :

DSPAV/RMF-KS



NIST SP 800-53

IA-5 (1) a

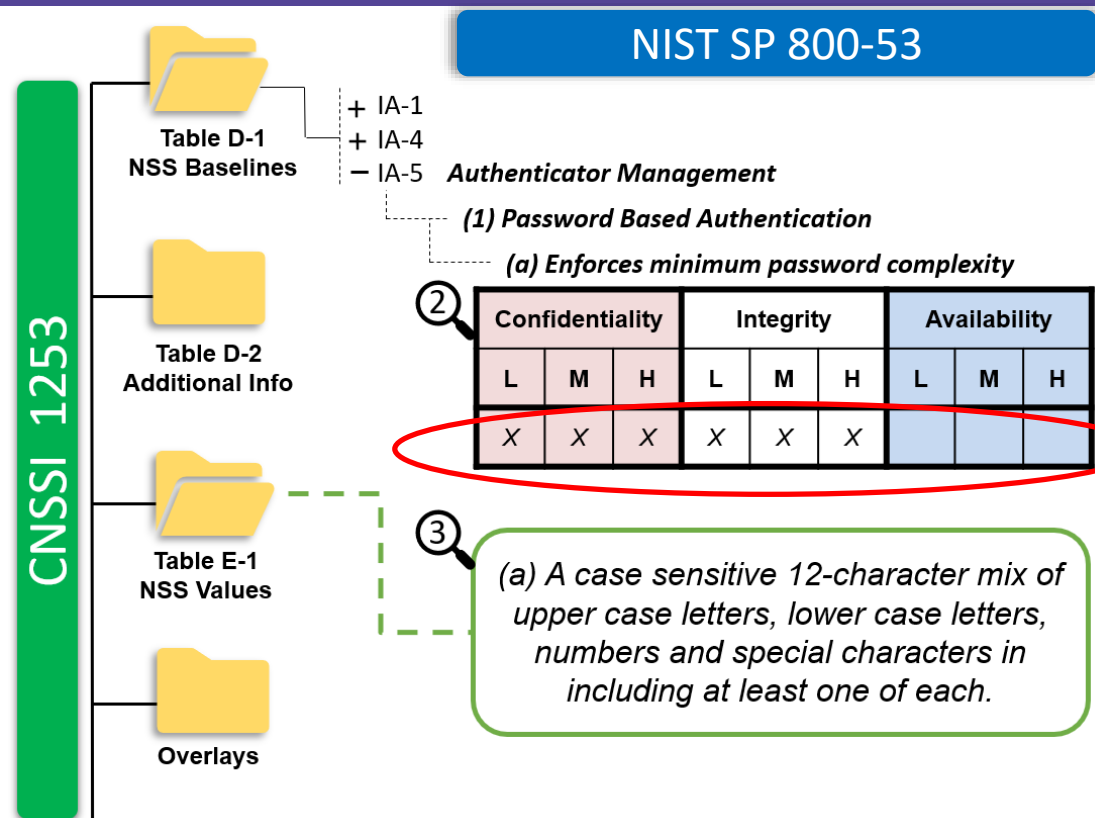
The information system: enforces minimum password complexity of

[Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];

CNSSI 1253



Modern STIG Source - Enhanced View



1. NIST SP 800-53
2. CNSSI 1253, Table D-1, "NSS Baselines"
3. CNSSI 1253, Table E-1, "NSS Values"
4. DSPAV / RMF-KS Values
5. DISA publishes Control Correlation Identifiers (CCI) for DoD



Converting Legacy STIGs to Modern STIGs

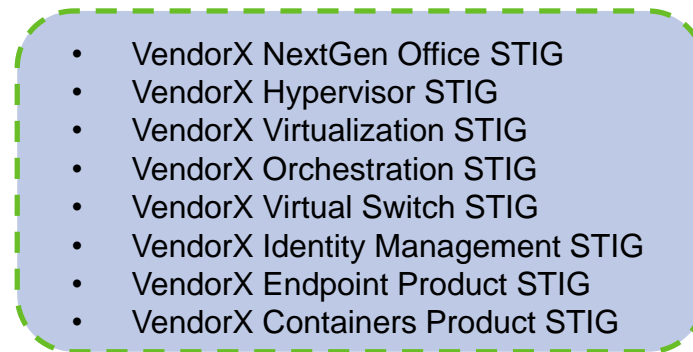
- Modern STIGs should be based on DSAWG-approved SRGs
- Requirements are not a 1-for-1 between the old and new references
- Goal for modern STIGs is to focus on technical CCI – configurations
- Modern STIGs will be less infrastructure and less policy based
- Modern STIGs promote the concepts of RMF

Program Level*

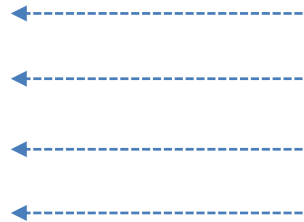


**No Policy STIGs at this level.*

Technology Specific**



*** Sample STIGs to support technology initiatives at this level.*





Status, Residual Legacy, Cleanup & Future

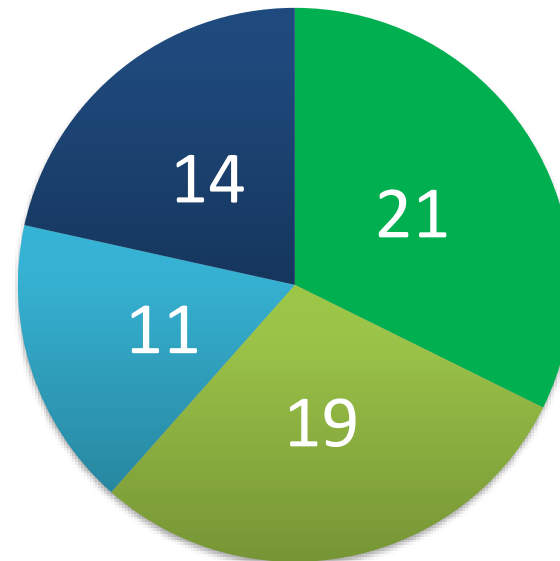
- Some legacy STIG products remain, but we're working on them
- Expect to see remaining legacy products move to sunset NLT CY2020

PENDING START

- Cisco Switch
- MFD and Printers
- NIPRNet DMZ
- SAN (storage)

STARTED

- Enclave T&D Zones
- Remote Access (all)
- VPN (all)
- Cisco Router (all)



■ Updated ■ Removed ■ Started ■ Pending



DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency



www.disa.mil



[/USDISA](https://www.facebook.com/USDISA)



[@USDISA](https://twitter.com/USDISA)

visit us

**DISA
Booth** **1929**

follow us



Facebook/USDISA



Twitter/USDISA

meet with us

Industry partners can request a meeting with DISA by completing a form at www.disa.mil/about/industry-partners.